ELSEVIER

Journal of Pure and Applied Algebra 94 (1994) 1–15

JOURNAL OF PURE AND APPLIED ALGEBRA

Semisimple algebras, Galois actions and group cohomology

Eli Aljadeff*,[a], Derek J.S. Robinson**,[b]

[a] *Department of Mathematics, Technion – Israel Institute of Technology, 32000 Haifa, Israel*
[b] *Department of Mathematics, University of Illinois, Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801, USA*

Communicated by K.W. Gruenberg; received 6 November 1992

Abstract

Let K be any field of characteristic $p > 0$ and let G be a finite group acting on K via a map τ. The skew group algebra $K_\tau G$ may be non-semisimple (precisely when $p||H|$, $H = \mathrm{Ker}\,\tau$).

We provide necessary conditions for the existence of a class $\alpha \in H^2(G, K^*)$ which "twists" the skew group algebra $K_\tau G$ into a semisimple crossed product $K_\tau^\alpha G$. Further, we give a thorough analysis of the converse problem namely whether these conditions are also sufficient for the existence of a "semisimple 2-cocycle". As a consequence we show this it is indeed so in many cases, in particular whenever G is a p-group.

1. Introduction

If G is a finite group and K is a field, the classical theorem of Maschke asserts that the group algebra KG is semisimple, i.e., its radical is zero, if and only if the characteristic of K either equals 0 or fails to divide $|G|$. Thus, if K has prime characteristic p and p divides $|G|$, then KG is not semisimple, the so-called modular case. In this article we are concerned with the possibility of "perturbing" the group algebra in the modular case in such a way as to produce a semisimple algebra.

Now there is a well-established way of perturbing a group algebra KG where K is any field and G any group. First one introduces an action of G on K, i.e., a homomorphism $\tau: G \to \mathrm{Aut}\,K$. Regarding $K^* = K\backslash\{0\}$ as G-module in the natural way, one chooses a cocycle α from $Z^2(G, K^*)$. Then the *crossed product*

$$K_\tau^\alpha G$$

* Corresponding author

** The second author was a visitor at the National University of Singapore during the period of this research.

SSDI 0022-4049(93)E0103-B

is defined as the (left) K-vector space with basis $\{u_x \mid x \in G\}$, the multiplication being given by the rule

$$(au_x)(bu_y) = ax(b)\alpha(x, y)\, u_{xy}$$

where $a, b \in K$, $x, y \in G$ and $x(b)$ denotes $\tau(x)(b)$. Here one can assume that u_1 is the identity element of the crossed product. It is well known that $K_\tau^\alpha G$ depends on α only up to its cohomology class, so that it is meaningful to write $K_\tau^\alpha G$ when α is an element of $H^2(G, K^*)$. For further information about crossed products the reader may consult [4].

If τ is the trivial homomorphism, i.e., G acts trivially on K, it is usual to omit the action and write the crossed product as

$$K^\alpha G,$$

the *twisted group algebra.* Similarly, if $\alpha = 0$, one simply writes

$$K_\tau G,$$

the *skew group algebra.*

Our first concern in this article is to find necessary and sufficient conditions on the pair (τ, α) for the crossed product $K_\tau^\alpha G$ to be semisimple when K is a field and G a finite group. In this case semisimplicity is equivalent to the global dimension being zero,

$$\text{gl.dim}(K_\tau^\alpha G) = 0.$$

The idea of twisting a group algebra to force semisimplicity is not a new one. Karpilovsky [3, Theorem 34.5] has given necessary and sufficient conditions for the twisted group algebra $K^\alpha G$ to be semisimple—see also [4, p. 186]. Our main contribution here is to use cohomological techniques to obtain more precise conditions for a general crossed product to be semisimple.

The following basic result has been established by Aljadeff and Rosset [1].

Theorem A. *Let G be a group and K a field. If τ is an action of G on K and $\alpha \in H^2(G, K^*)$, then*

$$\text{gl.dim}(K_\tau^\alpha G) \leq \text{gl.dim}(K_\tau G) \leq \text{gl.dim}(KG). \qquad \square$$

Thus the introduction of an action and a cocycle cannot increase the global dimension, which raises the possibility that $K_\tau^\alpha G$ may be semisimple even if KG is not. A point to keep in mind here is that when G is finite, $\text{gl.dim}(K_\tau^\alpha G) = 0$ or ∞.

There are two important reduction theorems which aid us in the task of deciding whether a crossed product is semisimple.

Theorem B [1, Theorem 3.2]. *Let G be a group, K a field, τ an action of G on K, and α an element of $H^2(G, K^*)$. Write $H = \text{Ker}\,\tau$. Then $K_\tau^\alpha G$ is semisimple if and only if $K^{\bar{\alpha}} H$ is semisimple where $\bar{\alpha}$ denotes the restriction of α to H.* $\square$

This effectively reduces the semisimplicity problem to the case of trivial action. The second reduction allows us to concentrate on p-groups.

Theorem C [4, p. 184]. *Let G be a finite group and K a field of characteristic $p > 0$. Denote by P a Sylow p-subgroup of G. Let τ be an action of G on K and let $\alpha \in H^2(G, K^*)$. Then $K_\tau^\alpha G$ is semisimple if and only if $K_{\bar\tau}^{\bar\alpha} P$ is semisimple where $\bar\tau$ and $\bar\alpha$ are the restrictions of τ and α to P.* □

It soon emerges from the theory that if $K^\alpha G$ is semisimple, then P must be abelian ([3, Theorem 34.5]; see also the proof of Theorem 2). Thus it is necessary to analyze the structure of $H^2(P, K^*)$ when P is a finite abelian p-group acting trivially on a field K of characteristic p.

Since $|P|$ annihilates the Schur multiplicator $M(P)$ and K^* has no p-elements, $\mathrm{Hom}(M(P), K^*) = 0$. Hence

$$H^2(P, K^*) \simeq \mathrm{Ext}\,(P, K^*)$$

by the Universal Coefficients Theorem. Writing

$$P = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$$

where x_i has order $p^{e_i} > 1$, we deduce that

$$H^2(P, K^*) \simeq \bigoplus_{i=1}^{r} K^*/(K^*)^{p^{e_i}}.$$

Thus each α in $H^2(P, K^*)$ is represented by an r-tuple

$$(a_1(K^*)^{p^{e_1}}, \ldots, a_r(K^*)^{p^{e_r}}), \tag{1}$$

with $a_i \in K^*$. More precisely, α arises from the 2-cocycle $\alpha_0 \in Z^2(P, K^*)$ defined by

$$\alpha_0(x_1^{s_1} \cdots x_r^{s_r}, x_1^{t_1} \cdots x_r^{t_r}) = a_1^{f_1} \cdots a_r^{f_r}$$

where

$$f_i = \begin{cases} 1 & \text{if } s_i + t_i \geq p^{e_i}, \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

The first question to be addressed is: which r-tuples give rise to elements $\alpha \in H^2(P, K^*)$ for which $K^\alpha P$ is semisimple?

Before giving the answer, we recall that if k is a subfield and U is a subset of a field K of characteristic p, then U is called *p-independent* over k if

$$k(K^p)(U) \neq k(K^p)(U_0)$$

whenever U_0 is a proper subset of U. If U is p-independent over k and also $K = k(K^p)(U)$, then U is called a *p-basis* of K over k. It is known that every p-independent subset is contained in a p-basis, and that all p-bases have the same

cardinal, which is called the *p-degree* of K over k. For these facts the reader is referred to [6, Section 4.3].

The following result answers the semisimplicity question for finite abelian p-groups and plays a central role in the theory.

Proposition 1. *Let P be a finite abelian p-group with $P = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle$ where $|x_i| = p^{e_i} > 1$. Let K be a field of characteristic p on which P acts trivially. Suppose that $\alpha \in H^2(P, K^*)$ is represented by the r-tuple $(a_1(K^*)^{p^{e_1}}, \ldots, a_r(K^*)^{p^{e_r}})$ with $a_i \in K^*$ as specified in* (1) *and* (2). *Then $K^\alpha P$ is semisimple if and only if $\{a_1, \ldots, a_r\}$ is p-independent over K^p.*

This is the basis for our first main result. The notation is that of (1) and (2).

Theorem 2. *Let G be a finite group and K a field of characteristic $p > 0$. Suppose that τ is an action of G on K with kernel H, and let $\alpha \in H^2(G, K^*)$. Let P be a Sylow p-subgroup of H. Then $K_\tau^\alpha G$ is semisimple if and only if the following hold:*

(i) *$|H'|$ is prime to p, so that P is abelian;*

(ii) *$\mathrm{res}_P^G(\alpha)$ is represented by an r-tuple $(a_1(K^*)^{p^{e_1}}, \ldots, a_r(K^*)^{p^{e_r}})$ such that $\{a_1, \ldots, a_r\}$ is p-independent over K^p.*

The twisting problem

Next we change our point of view and consider the problem: if K is a field of characteristic $p > 0$, G is a finite group and τ is an action of G on K, when does there exist an α in $H^2(G, K^*)$ such that $K_\tau^\alpha G$ is semisimple? In short, we seek to twist the skew group algebra $K_\tau G$ to make it semisimple.

Let $H = \mathrm{Ker}\,\tau$ and denote by P a Sylow p-subgroup of H. Then Theorem 2 shows that the following conditions are necessary if there is to be an α in $H^2(G, K^*)$ such that $K_\tau^\alpha G$ is semisimple:

(i) H' is a p'-group;

(ii) the rank of P does not exceed the p-degree of K over K^p.

The question posed here is whether conditions (i) and (ii) are sufficient to imply the existence of an α in $H^2(G, K^*)$ for which $K_\tau^\alpha G$ is semisimple. We shall refer to this as the *twisting problem*. While it has the appearance of a difficult problem in general, there is an affirmative answer of course when τ is a faithful action; indeed $K_\tau^\alpha G$ will be semisimple whatever α is chosen, by Theorem 2. (In fact, $K_\tau^\alpha G$ is even simple.) The answer is also positive at the other extreme, when τ is trivial; this will follow from Theorem 5 below. While the twisting problem remains open in general, we are able to give a thorough analysis of it, and to resolve it in some important cases.

In the course of our analysis we have come across some results of independent interest, in particular regarding the "Galois modules" $K^*/(K^*)^{p^e}$. The first of these is the following theorem.

Theorem 3. *Let K be a field of characteristic $p > 0$, Q a finite subgroup of* Aut K, *and e a positive integer. Then the $\mathbb{Z}_{p^e}$ Q-module $K^*/(K^*)^{p^e}$ has free submodule of all finite ranks not exceeding the p-degree of K over K^p.*

Then, by using a simple device for embedding modules in free modules, we deduce the following.

Theorem 4. *Let K be a field of characteristic $p > 0$, and Q a finite subgroup of* Aut K. *If M is any finite $\mathbb{Z}_{p^e}$ Q-module whose $\mathbb{Z}$-rank does not exceed the p-degree of K over K^p, then M is isomorphic with a submodule of the $\mathbb{Z}_{p^e}$ Q-module $K^*/(K^*)^{p^e}$.*

The point of this result is that it enables us to construct non-zero elements of $H^2(H, K^*)^Q$ where $H = \operatorname{Ker}\tau$ and $Q = \operatorname{Im}\tau$, as one can see from Proposition 9 below. Such elements are essential in any attempt to extend an element of $H^2(H, K^*)$ to G. However, we need to find elements α of $H^2(H, K^*)$ for which $K^\alpha H$ is semisimple, so there is a further condition to be satisfied. It turns out that the condition can be satisfied if the Q-module $H/O_{p'}(H)$ has a property which we have named triangularity.

A Q-module M is called *triangular* if there is a series of submodules

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = M$$

such that each M_{i+1}/M_i is a cyclic group. Such modules occur naturally; for example, M will be triangular if both M and Q are finite p-groups.

Assuming that we have found an element α of $H^2(H, K^*)^Q$ for which $K^\alpha G$ is semisimple, we still need to verify that α belongs to the kernel of a certain differential in a spectral sequence if α is to extend to G (see Lemma 8). Fortunately, the construction of our cocycle α is sufficiently explicit that this can be done directly.

Our principal conclusions on the twisting problem are summarized in the following result.

Theorem 5. *Let K be a field of characteristic $p > 0$, G a finite group, and $\tau: G \to$ Aut K an action of G on K. Put $H = \operatorname{Ker}\tau$ and $Q = \operatorname{Im}\tau$. Then there is an α in $H^2(G, K^*)$ such that $K^\alpha_\tau G$ is semisimple provided that the following conditions are satisfied:*

(i) *H' is a p'-group,*

(ii) *the rank of $H/O_{p'}(H)$ does not exceed the p-degree of K over K^p,*

(iii) *$H/O_{p'}(H)$ is a triangular Q-module.*

For example, (iii) will certainly hold if the group G is supersoluble, or, more generally, if H is *supersolubly embedded* in G, i.e., there is a chain of G-admissible subgroups $1 = H_0 < H_1 < \cdots < H_n = H$ such that each H_{i+1}/H_i is cyclic.

Another special case of interest occurs when K is a local field; then condition (ii) implies that $H/O_{p'}(H)$ is cyclic, so that (iii) holds automatically, and we obtain the following corollary.

Corollary. *Let K be a local field of characteristic $p > 0$, G a finite group, and $\tau: G \to \mathrm{Aut}\, K$ an action of G on K with kernel H. Then there is an α in $H^2(G, K^*)$ such that $K_\tau^\alpha G$ is semisimple if and only if H' is a p-group and $H/O_{p'}(H)$ is cyclic.* □

Thus the twisting problem has a positive solution for local fields.

We would like to acknowledge Jack Sonn for very useful conversations he had with the first author.

2. Criteria for semisimplicity

Our aim in this section is to prove Theorem 2. We begin with a condition for p-independence that does not seem to appear in the literature.

Lemma 6. *Let K be a field of characteristic $p > 0$, and let $a_1, \ldots, a_r$ be elements of K. Then $\{a_1, \ldots, a_r\}$ is p-independent over K^p if and only if, for every r-tuple $(e_1, \ldots, e_r)$ of positive integers, $a_{i+1} \notin K_i^p$ for $i = 0, 1, \ldots, r-1$, where $K_i = K(a_1^{1/p^{e_1}}, \ldots, a_i^{1/p^{e_i}})$.*

Proof. If $\{a_1, \ldots, a_r\}$ is not p-independent, it is straightforward to show that there is an i for which $a_{i+1} \in K^p(a_1, \ldots, a_i)$. Then $a_{i+1} \in (K(a_1^{1/p}, \ldots, a_i^{1/p}))^p$, so the condition does not hold.

Conversely, assume that $\{a_1, \ldots, a_r\}$ is p-independent. If the condition is invalid, there is an r-tuple $(e_1, \ldots, e_r)$ such that $a_{i+1} \in K_i^p$ where $0 \le i < p$. Here we can suppose that i is chosen minimal subject to this property. Hence there is an equation

$$a_{i+1} = \sum b_{s_1 \ldots s_i}^p a_1^{s_1/p^{e_1-1}} \cdots a_i^{s_i/p^{e_i-1}}$$

where $b_{s_1 \ldots s_i} \in K$ and the sum is over all $(s_1, \ldots, s_i)$ with $0 \le s_j < p^{e_j}$. Write $s_j = d_j + c_j p^{e_j-1}$ where d_j, c_j are integers and $0 \le d_j < p^{e_j-1}$. Then

$$\begin{aligned} a_{i+1} &= \sum (b_{s_1 \ldots s_i}^p a_1^{c_1} \cdots a_i^{c_i}) a_1^{d_1/p^{e_1-1}} \cdots a_1^{d_i/p^{e_i-1}} \\ &= f(a_1^{1/p^{e_1-1}}, \cdots, a_i^{1/p^{e_i-1}}), \end{aligned}$$

where f is a polynomial in $t_1, \ldots, t_i$ over $K^p(a_1, \ldots, a_i)$. By p-independence f is not constant, so there is a largest $j \le i$ such that t_j actually occurs in f. Then $a_j^{1/p^{e_j-1}}$ is a root of a polynomial over $L = K(a_1^{1/p^{e_1-1}}, \ldots, a_{j-1}^{1/p^{e_j-1}})$ having degree less than p^{e_j-1}. Therefore $t^{p^{e_j-1}} - a_j$ is reducible over L, from which it follows that $a_j \in L^p \subseteq K_{j-1}^p$, contradicting the minimality of i. □

Proof of Proposition 1. In the first place there is an obvious isomorphism

$$K^\alpha P \simeq K[t_1, \ldots, t_r]/(t^{p^{e_1}} - a_1, \ldots, t^{p^{e_r}} - a_r).$$

If $K^\alpha P$ is semisimple, then $a_{i+1} \notin K^p(a_1, \ldots, a_i)$, otherwise there would be a non-zero nilpotent element in $K^\alpha P$. Hence $\{a_1, \ldots, a_r\}$ is p-independent over K^p.

Conversely, assume that $a_1, \ldots, a_r$ are p-independent. Then $a_{i+1} \notin K_i^p$ where $K_i = K(a_1^{1/p^{e_1}}, \ldots, a_i^{1/p^{e_i}})$ by Lemma 6. It follows that $t_i^{p^{e_{i+1}}} - a_{i+1}$ is irreducible over K_i. Therefore $K^\alpha P \simeq K_r$, and $K^\alpha P$ is semisimple. (Notice that $K^\alpha P$ is a purely inseparable field extension of K.) □

Proof of Theorem 2. Assume that $K_\tau^\alpha G$ is semisimple. Then Theorem B shows that $K^\alpha H$ is semisimple (where α is also used to denote the restriction to H). By naturality of the universal coefficients sequence, there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ext}(H_{\mathrm{ab}}, K^*) & \xrightarrow{\theta} & H^2(H, K^*) & \xrightarrow{\phi} & \mathrm{Hom}(M(H), K^*) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \mathrm{res}_P^H} & & & & \\ 0 & \longrightarrow & \mathrm{Ext}(P_{\mathrm{ab}}, K^*) & \longrightarrow & H^2(P, K^*) & \longrightarrow & \mathrm{Hom}(M(P), K^*) & \longrightarrow & 0 \end{array}$$

Note here that $\mathrm{Hom}(M(H), K^*)$ has no p-elements.

Let $\alpha = \alpha_p + \alpha_{p'}$ be the decomposition of α into its p- and p'-components. Then $\phi(\alpha_p) = 0$, so that $\alpha_p \in \mathrm{Im}\,\theta$ and $\mathrm{res}_{H'}^H(\alpha_p) = 0$. Also $\mathrm{res}_P^H(\alpha_{p'}) = 0$. Therefore $\mathrm{res}_{P \cap H'}^H(\alpha) = 0$, which shows that

$$K^\alpha(P \cap H') = K(P \cap H').$$

Now by [1, Proposition 4.1] we see that $K(P \cap H')$ is also semisimple. Therefore $P \cap H' = 1$ and $|H'|$ is prime to p. The necessity of (ii) follows from Theorem C and Proposition 1.

Conversely, if (i) and (ii) hold, then $K^\alpha P$ is semisimple by Proposition 1, and Theorems C and B show that $K_\tau^\alpha G$ is semisimple. □

3. Reductions for the twisting problem

Let $\tau: G \to K$ be a given action of a finite group G on a field K of characteristic $p > 0$. Write $H = \mathrm{Ker}\,\tau$ and $Q = \mathrm{Im}\,\tau$, and let P be a Sylow p-subgroup of H. We assume the validity of the two conditions which are known to be necessary for the existence of an α in $H^2(G, K^*)$ such that $K_\tau^\alpha G$ is semisimple:

(i) H' is a p'-group,

(ii) the rank of P does not exceed the p-degree of K over K^p.

Then Proposition 1 shows that there is an α in $H^2(P, K^*)$ such that $K^\alpha P$ is semisimple. For if P has rank, r, we can find a p-independent subset $\{a_1, \ldots, a_r\}$, and then construct α using (1) and (2).

It must still be determined if some such α extends to G, i.e., if $\alpha \in \mathrm{Im}(\mathrm{res}_P^G)$. For, if β is an extension of α to G, then $K_\tau^\beta G$ will be semisimple by Theorems B and C.

The first reduction which we make is to the case where $H = P$ is an abelian p-group. Condition (i) implies that P has a normal p'-complement N in H, and $N \lhd G$. Put $\bar{G} = G/N$ and $\bar{H} = H/N$; let $\bar{\tau}: \bar{G} \to \mathrm{Aut}\,K$ be the induced action of $\bar{G}$ on K. The result needed is the following.

Proposition 7. *With the above notation, there is an α in $H^2(G, K^*)$ such that $K_\tau^\alpha G$ is semisimple if and only if there is an $\bar{\alpha}$ in $H^2(\bar{G}, K^*)$ making $K_\tau^{\bar{\alpha}}\bar{G}$ semisimple.*

Proof. Consider the commutative diagram

$$\begin{array}{ccc} H^2(G,K^*)_p & \xrightarrow{\text{res}} & H^2(P,K^*) \\ & \text{inf} & \\ H^2(\bar{G},K^*)_p & \longrightarrow & H^2(P,K^*) \end{array}$$

Here subscript p denotes the p-component. Since N is a p'-group, the spectral sequence associated with $1 \to N \to G \to \bar{G} \to 1$ collapses on p-components. Therefore inf induces an isomorphism on p-components. Finally, if $\bar{\alpha} \in H^2(\bar{G}, K^*)$ and $\inf(\bar{\alpha}) = \alpha$, then $K_\tau^{\bar{\alpha}}\bar{G}$ is semisimple if and only if $K^\alpha P$ is semisimple; and the same holds for $K_\tau^\alpha G$. □

Because of Proposition 7, we shall make the assumption that $H = P$ is an abelian p-group. Since $\mathrm{Hom}(P, K^*) = 0$, the spectral sequence associated with $1 \to P \to G \to Q \to 1$ yields

$$\mathrm{Im}(\mathrm{res}_P^G) = \mathrm{Ker}(d: H^2(P, K^*)^Q \to H^3(Q, K^*)).$$

Thus we may state the following.

Lemma 8. *Let $\alpha \in H^2(P, K^*)$. Then α extends to G in such a way that $K_\tau^\alpha G$ is semisimple if and only if $K^\alpha P$ is semisimple and α belongs to the kernel of the differential $d: H^2(P, K^*)^Q \to H^3(Q, K^*)$.* □

The next step is to replace $H^2(P, K^*)^Q$ by a more easily understood homomorphism group, and establish thereby the crucial connection with embeddings in $K^*/(K^*)^{p^e}$.

Proposition 9. *Let K be a field of characteristic $p > 0$ and Q a finite subgroup of* Aut K. *If M is any $\mathbb{Z}_{p^e}Q$-module, then*

$$H^2(M, K^*)^Q \simeq \mathrm{Hom}_{\mathbb{Z}_{p^e}Q}(M, K^*/(K^*)^{p^e})$$

where M acts trivially on K^*.

Proof. Consider the exact sequence of abelian groups $1 \to K^* \xrightarrow{\theta} K^* \to K^*/(K^*)^{p^e} \to 1$ where $\theta(x) = x^{p^e}$. Applying $\mathrm{Hom}_{\mathbb{Z}}(M, -)$, we obtain the exact sequence

$$0 \to \mathrm{Hom}(M, K^*/(K^*)^{p^e}) \to \mathrm{Ext}(M, K^*) \xrightarrow{\theta_*} \mathrm{Ext}(M, K^*)$$

since $\mathrm{Hom}(M, K^*) = 0$. But $\theta_* = 0$ since $p^e M = 0$. Therefore

$$\mathrm{Hom}(M, K^*/(K^*)^{p^e}) \simeq \mathrm{Ext}(M, K^*) \simeq H^2(M, K^*)$$

by the Universal Coefficients Theorem and $\mathrm{Hom}(H_2 M, K^*) = 0$. The isomorphisms here are of Q-modules, with Q acting diagonally. The result now follows on taking Q-fixed points. □

Proposition 9 shows that we have to study $\mathbb{Z}_{p^e}Q$-homomorphisms from M to $K^*/(K^*)^{p^e}$ in order to understand $H^2(M, K^*)^Q$. With this in mind, let us write $M = \langle x_1\rangle \oplus \cdots \oplus \langle x_r\rangle$ where $|x_i| = p^{e_i}$ and $0 < e_i \leq e$. If $\phi \in \mathrm{Hom}_{\mathbb{Z}_{p^e}Q}(M, K^*/(K^*)^{p^e})$, then

$$\phi(x_i) = b_i^{p^{e-e_i}}(K^*)^{p^e} \tag{3}$$

where $b_i \in K^*$. So there is a corresponding r-tuple $(b_1, \ldots, b_r)$ where b_i is uniquely determined modulo $(K^*)^{p^{e_i}}$. Now an α in $H^2(M, K^*)$ also determines an r-tuple of this sort, as described by (1) and (2). It is routine to verify that the corresponding maps are homomorphisms which make the following diagram commute

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}_{p^e}Q}(M, K^*/(K^*)^{p^e}) & \simeq & H^2(M, K^*)^Q \\ \downarrow & \swarrow & \\ \bigoplus_{i=1}^{r} K^*/(K^*)^{p^{e_i}} & & \end{array}$$

Because of Proposition 1 we are able to deduce the following.

Lemma 10. *With the previous notation, let ϕ in $\mathrm{Hom}_{\mathbb{Z}_{p^e}Q}(M, K^*/(K^*)^{p^e})$ correspond to α in $H^2(M, K^*)^Q$. Then $K^\alpha M$ is semisimple if and only if the elements $b_1, \ldots, b_r$ defined in (3) are p-independent over K^p.* □

It is clear that $b_1, \ldots, b_r$ cannot be p-independent if ϕ is not injective. This focuses our attention on the possibility of embedding M in $K^*/(K^*)^{p^e}$, which is the topic of the next section.

4. Module embeddings

The first step in the process of embedding a $\mathbb{Z}_{p^e}Q$-module M in a Galois module $K^*/(K^*)^{p^e}$ is to find free submodules with large enough rank. The following result is fundamental.

Theorem 11. *Let K be a field of characteristic $p > 0$, Q a finite subgroup of* Aut K, *and e a positive integer. Then the $\mathbb{Z}_{p^e}Q$-module $K^*/(K^*)^{p^e}$ has free submodules of all finite ranks not exceeding the p-degree of K over K^p.*

The proof is preceded by two simple results which may be known.

Lemma 12. *Let $a_1, \ldots, a_r$ be elements of a field of characteristic $p > 0$. Then $a_1, \ldots, a_r$ are p-independent over K^p if and only if the monomials $a_1^{i_1} a_2^{i_2} \cdots a_r^{i_r}$, $0 \leq i_j < p$, are linearly independent over K^p.*

Proof. If the monomials are linearly dependent, there is an $s \leq r$ and a non-zero polynomial g of degree less than p over $L = K^p(a_1, \ldots, a_{s-1})$ such that $g(a_s) = 0$. Put $h = t^p - a_s^p \in L[t]$; then h is reducible since $\deg(g) < p$. Consequently $a_s \in L$ and the elements $a_1, \ldots, a_r$ are not p-independent. Conversely, if these elements are not p-independent, it is clear that the monomials must be linearly dependent over K^p. □

Lemma 13. *Let K be a finite Galois extension of a field k of characteristic $p > 0$, and let A be a subset of k which is p-independent over k^p. Then A is p-independent over K^p. If A is a p-basis of k over k^p, then it is a p-basis of K over K^p.*

Proof. If the first claim is false, there is a smallest integer $r > 0$ for which there exist r elements $a_1, \ldots, a_r$ of A that are p-dependent over K^p. Then $a_r \in K^p(a_1, \ldots, a_{r-1})$ and

$$a_r = \sum_{0 \leq i_j < p} b_{i_1 \ldots i_{r-1}}^p \, a_1^{i_1} \cdots a_{r-1}^{i_{r-1}} \tag{4}$$

where $b_{i_1 \ldots i_{r-1}} \in K$. Now the monomials $a_1^{i_1} \cdots a_{r-1}^{i_{r-1}}$ $(0 \leq i_j < p)$, are linearly independent over K^p; otherwise $a_1, \ldots, a_{r-1}$ are p-dependent over K^p, by Lemma 12, contradicting the choice of r. Applying $\sigma \in \mathrm{Gal}(K/k)$ to the equality (4), we conclude that σ must fix each $b_{i_1 \ldots i_{r-1}}$, so that these coefficients belong to k, which is impossible.

Now assume that A is a p-basis of k and put $L = K^p(A)$; thus $k \subseteq L \subseteq K$ since $k = k^p(A)$. Hence K is Galois over L. If $x \in K \setminus L$, then $t^p - x^p$ is irreducible over L, so it is inseparable. Therefore $K = L$ and A is a p-basis of K. □

Proof of Theorem 11. Let $k = K^Q$, the fixed field of Q; thus K is a finite Galois extension of k and $Q = \mathrm{Gal}(K/k)$. By Lemma 13 the p-degree of K equals the p-degree of k, and this can be assumed positive. Choose a positive integer r not exceeding the p-degree of K. Then there exist r elements $b_1, \ldots, b_r$ of k which are p-independent over K^p. Also there is an element z in K such that $\sigma(z) \neq z$ if $1 \neq \sigma \in Q$.

We aim to show that it is possible to choose $b_1, \ldots, b_r$ in such a way that the elements

$$(1 + b_i z^p)(K^*)^{p^e}, \quad i = 1, 2, \ldots, r,$$

form the basis of a free $\mathbb{Z}_{p^e}Q$-submodule of $K^*/(K^*)^{p^e}$. Now there are only finitely many non-trivial linear $\mathbb{Z}_{p^e}Q$-relations that could hold between these elements. Moreover, if $0 \neq u \in k^p$ and $a_i = b_i u$, then $a_1, \ldots, a_r$ are also p-independent over K^p. Therefore we can suppose that there exist integers $d_{\sigma i}$ satisfying $0 \leq d_{\sigma i} < p^e$, and not all zero, such that for infinitely many u in k^p the relation

$$\prod_{i=1}^{r} \prod_{\sigma \in Q} (\sigma(1 + a_i z^p))^{d_{\sigma i}} \in (K^*)^{p^e}$$

holds, with $a_i = b_i u$.

If p divides every $d_{\sigma i}$, then we can take pth roots and use induction on e. Thus we reduce to the case $e = 1$, when

$$\prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{d_{\sigma i}} \in (K^*)^p$$

with $0 \leq d_{\sigma i} < p$.

Let us write

$$c_i = \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{d_{\sigma i}} = f_{0i} + f_{1i} a_i + \cdots + f_{p-1\,i} a_i^{p-1}$$

where f_{ji} is a polynomial in a_i^p over the field $L = \mathbb{Z}_p(\sigma(z)^p \mid \sigma \in Q)$. Expand the product $c_1 c_2 \cdots c_r$ and equate the coefficients of the resulting monomials to 0, using Lemma 12. We obtain

$$f_{j_1 1} f_{j_2 2} \cdots f_{j_r r} = 0$$

for all $(j_1, \ldots, j_r) \neq (0, \ldots, 0)$.

We claim that there is an i for which $f_{ji} = 0$ for all $j > 0$. This is obvious if $r = 1$, so assume that $r > 1$. If $f_{0r} \neq 0$, then $f_{j_1 1} \cdots f_{j_{r-1} r-1} = 0$, for all $(j_1, \ldots, j_{r-1}) \neq (0, \ldots, 0)$, and the assertion is true by induction on r. On the other hand, if $f_{0r} = 0$ but $f_{jr} \neq 0$ for some $j > 0$, then $f_{j_1 1} \cdots f_{j_{r-1} r-1} = 0$ for all $(j_1, \ldots, j_{r-1})$, and again the claim follows.

We have now reached the position where

$$c_i = \prod_{\sigma} (1 + a_i \sigma(z)^p)^{d_{\sigma i}} = f_{0i}(a_i^p),$$

so that a_i is a root of the polynomial $g_i = \prod_\sigma (1 + t\sigma(z)^p)^{d_{\sigma i}} - f_{0i}(t^p)$ over L. Since we can choose $a_i = b_i u$ in infinitely many ways, $g_i = 0$ and

$$\prod_{\sigma \in Q} (1 + t\sigma(z)^p)^{d_{\sigma i}} = f_{0i}(t^p). \tag{5}$$

Assume that some $d_{\sigma i} \neq 0$. There is no loss of generality in supposing that $\sigma = 1$ and $d_{1i} = 1$. Now differentiate (5) and put $t = -1/z^p$; a contradiction ensues since $\sigma(z) \neq z$ if $1 \neq \sigma \in Q$. It follows that $d_{\sigma i} = 0$ for all σ. We can now use induction on r to conclude that $d_{\sigma j} = 0$ for all σ and j. □

The next step is to show how to embed a module in a free module.

Proposition 14. *Let Q be a finite group and M a finite left $\mathbb{Z}_{p^e}Q$-module with $\mathbb{Z}$-rank r. Then M is isomorphic with a submodule of a free $\mathbb{Z}_{p^e}Q$-module of rank r.*

Proof. Let $M = \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_r}}$ where $0 < e_i \leq e$. By [2, p. 611] there is an isomorphism of right $\mathbb{Z}_{p^e}Q$-modules

$$\theta_0 : \mathrm{Hom}_{\mathbb{Z}_{p^e}}(M, \mathbb{Z}_{p^e}) \to \mathrm{Hom}_{\mathbb{Z}_{p^e}}(M, \mathbb{Z}_{p^e}Q)$$

given by the rule $\theta_0(\xi)(a) = \sum_{\sigma\in Q} \xi(\sigma^{-1}a)\sigma$ where $\xi \in \mathrm{Hom}_{\mathbb{Z}_{p^e}}(M, \mathbb{Z}_{p^e})$ and $a \in M$. We use this to manufacture a $\mathbb{Z}_{p^e}Q$-isomorphism

$$\theta: \mathrm{Hom}_{\mathbb{Z}_{p^e}}(M, \oplus(\mathbb{Z}_{p^e})^r) \to \mathrm{Hom}_{\mathbb{Z}_{p^e}Q}(M, \bigoplus(\mathbb{Z}_{p^e}Q)^r).$$

This is defined by $(\theta(\xi)(a))_i = \sum_\sigma \xi_i(\sigma^{-1}a)\sigma$ where $\xi \in \mathrm{Hom}_{\mathbb{Z}_{p^e}}(M, \bigoplus(\mathbb{Z}_{p^e})^r)$ and $a \in M$. Here ξ_i is the composite of ξ with the projection of $\bigoplus(\mathbb{Z}_{p^e})^r$ onto its ith direct summand. Now take ξ to be a homomorphism which maps $\mathbb{Z}_{p^{e_i}}$ injectively into the ith summand $\mathbb{Z}_{p^e}$ for each i. It is easy to check that $\theta(\xi)$ is injective, so it is a $\mathbb{Z}_{p^e}Q$-embedding of M in $\bigoplus(\mathbb{Z}_{p^e}Q)^r$. □

Combining Theorem 11 and Proposition 14, we obtain at once the following theorem.

Theorem 15. *Let K be a field of characteristic $p > 0$, Q a finite subgroup of* Aut K, *and e a positive integer. If M is any finite $\mathbb{Z}_{p^e}Q$-module whose $\mathbb{Z}$-rank does not exceed the p-degree of K over K^p, then M is isomorphic with a submodule of the $\mathbb{Z}_{p^e}Q$-module $K^*/(K^*)^{p^e}$.* □

It is essential to have on hand an explicit description of the embedding $\phi: M \to K^*/(K^*)^{p^e}$ which is provided by the proof of Theorem 15. This is given by

$$\phi(x) = \prod_{i=1}^{r} \prod_{\sigma\in Q} (1 + a_i\sigma(z)^p)^{(\sigma^{-1}x)_i p^{e-e_i}} (K^*)^{p^e} \tag{6}$$

where $M = \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_r}}$, $0 < e_i \leq e$, and the subscript i denotes the i-component in $\mathbb{Z}_{p^{e_i}}$. Of course z and the a_i have to be chosen appropriately, as in the proof of Theorem 11.

***p*-completions.** We pause to mention an interesting property of the p-completion of the module K^*. Let Q be a finite subgroup of Aut K where K is a field of characteristic $p > 0$. Suppose that M is a Q-lattice with $\mathbb{Z}$-rank not exceeding the p-degree of K over K^p. Choose and fix a basis of M, and from this derive the obvious basis for $M_e = M/p^eM$. By Theorem 15 there is a $\mathbb{Z}_{p^e}Q$-embedding ϕ_e of M_e in $K_e^* = K^*/(K^*)^{p^e}$ where ϕ_e is given by (6). It is easily seen that the maps ϕ_e are compatible, so that $\phi = (\phi_e)$ is an injective morphism of inverse systems from (M_e) to (K_e^*). Since $\varprojlim$ is left exact, there is an induced injective homomorphism of p-completions, $\hat{\phi}: \hat{M} \to (\hat{K}^*)$. Also M embeds in $\hat{M}$, so we have the following theorem.

Theorem 16. *Let Q be a finite subgroup of* Aut K *where K is a field of characteristic $p > 0$. Then the p-completion K^* contains a copy of every Q-lattice whose $\mathbb{Z}$-rank does not exceed the p-degree of K over K^p.* □

5. Semisimple embeddings

Having demonstrated the existence of module embeddings $\phi: M \to K^*/(K^*)^{p^e}$, we must now consider whether ϕ can be chosen so that $K^\alpha M$ is semisimple, where α is the element of $H^2(M, K^*)$ that corresponds to ϕ. As usual K is a field of characteristic $p > 0$, Q is a finite subgroup of Aut K, and M is a finite $\mathbb{Z}_{p^e}Q$-module with $\mathbb{Z}$-rank not exceeding the p-degree of K.

Let $M = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$ where $|x_i| = p^{e_i} > 1$. Writing

$$\phi(x_j) = b_j^{e-e_j}(K^*)^{p^e}, \tag{7}$$

we see from (6) that we can assume

$$b_j = \prod_{i=1}^{r} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}x_j)i} \tag{8}$$

where $z \in K$ satisfies $\sigma(z) \neq z$ for $\sigma \in Q$, and $\{a_1, \ldots, a_r\}$ is a suitable set of p-independent elements of $k = K^Q$.

Now by Lemma 10 $K^\alpha M$ is semisimple if and only if $b_1, \ldots, b_r$ are p-independent. The question is whether it is possible to choose the basis $x_1, \ldots, x_r$ of M so that this is true. When M is triangular, such a choice is always possible.

Theorem 17. *Let K be a field of characteristic $p > 0$, Q a finite subgroup of* Aut K, *and M a finite $\mathbb{Z}_{p^e}Q$-module with $\mathbb{Z}$-rank not exceeding the p-degree of K over K^p. If M is triangular, then there is an α in $H^2(M, K^*)^Q$ such that $K^\alpha M$ is semisimple.*

The proof is preceded by an elementary property of triangular modules.

Lemma 18. *Let Q be a group and M a finite Q-module whose underlying group is a p-group. Assume that M is a triangular module. Then there are elements $x_1, \ldots, x_r$ such that $M = \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle$, $|x_i| \leq |x_{i+1}|$ and $\sigma x_i \in \langle x_1, \ldots, x_i \rangle + pM$ for $i = 1, 2, \ldots, r$ and all $\sigma \in Q$.*

Proof. If $pM = 0$, let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ be a series of submodules with M_{i+1}/M_i cyclic. Choose x_i from $M_i \backslash M_{i-1}$; then $x_1, \ldots, x_r$ is a basis of M of the type sought. Assume now that $pM \neq 0$, and put $L = \{a \in M \mid pa = 0\}$. By induction on $|M|$ there exist elements $y_1, \ldots, y_s$ such that

$$M/L = \langle y_1 + L \rangle \oplus \cdots \oplus \langle y_s + L \rangle, \quad |y_i + L| \leq |y_{i+1} + L|$$

and $\sigma y_i \in \langle y_1, \ldots, y_i \rangle + L + pM$ for σ in Q and $i = 1, 2, \ldots, s$. If $|y_i| = p^{e_i}$, then $e_i > 1$ and $|y_i + L| = p^{e_i - 1}$; thus $e_i \leq e_{i+1}$.

We show first that $y_1, \ldots, y_s$ are $\mathbb{Z}$-independent. Indeed, if $\sum_i n_i y_i = 0$, then p divides n_i. Hence $\sum_i p(n_i/p)y_i = 0$ and $\sum (n_i/p)y_i \in L$. It follows that $n_i y_i = 0$ for all i.

Next we have $M = L + \langle y_1, \ldots, y_s\rangle$, so $pM \cap L = \langle p^{e_1-1}y_1\rangle \oplus \cdots \oplus \langle p^{e_s-1}y_s\rangle$ since $e_i > 1$. Let $z_1 + (pM \cap L), \ldots, z_t + (pM \cap L)$ be a basis of the required type for the triangular module $L/pM \cap L$. Then

$$L = \langle z_1\rangle \oplus \cdots \oplus \langle z_t\rangle \oplus \langle p^{e_1-1}y_1\rangle \oplus \cdots \oplus \langle p^{e_s-1}y_s\rangle,$$

from which it follows that M is the sum of the $\langle z_i\rangle$ and the $\langle y_j\rangle$. In fact this sum is direct. For if there is a relation $\sum_i l_i z_i + \sum_j m_j y_j = 0$, then $\sum_j m_j y_j \in L$ and p^{e_j-1} divides m_j. Hence $\sum_i l_i z_i + \sum_j (m_j/p^{e_j-1})p^{e_j-1}y_j = 0$, which implies that $l_i z_i = 0 = m_j y_j$ for all i and j. Therefore

$$M = \langle z_1\rangle \oplus \cdots \oplus \langle z_t\rangle \oplus \langle y_1\rangle \oplus \cdots \oplus \langle y_s\rangle.$$

Finally, if $\sigma \in Q$, we have

$$\sigma z_i \in \langle z_1, \ldots, z_i\rangle + (pM \cap L) \subseteq \langle z_1, \ldots, z_i\rangle + pM,$$

and also,

$$\sigma y_j \in \langle y_1, \ldots, y_j\rangle + L + pM = \langle z_1, \ldots, z_t, y_1, \ldots, y_j\rangle + pM$$

since $e_j > 1$. Thus $z_1, \ldots, z_t, y_1, \ldots, y_s$ is a basis of M of the required type. □

Remark. Simple examples show that one cannot expect to find a basis $x_1, \ldots, x_r$ such that $\sigma x_i \in \langle x_1, \ldots, x_i\rangle$ for all $\sigma \in Q$, $i = 1, \ldots, r$.

Proof of Theorem 17. Let $x_1, \ldots, x_r$ be basis for M of the type specified in Lemma 18. Choose elements $z, a_1, \ldots, a_r$ in K as in the proof of Theorem 11. Let $\phi: M \to K^*/(K^*)^{p^e}$ be the embedding (6) produced by Theorem 11 and Proposition 14, with corresponding elements b_j given by (7) and (8). We must show that the b_j are p-independent.

By choice of the x_j, we have $(\sigma^{-1}x_j)_i \equiv 0 \pmod p$ if $j < i$. It follows from (8) that

$$b_j \equiv \prod_{i=1}^{j} \prod_{\sigma \in Q} (1 + a_i \sigma(z)^p)^{(\sigma^{-1}x_j)_i} \mod (K^*)^p,$$

and consequently $b_j \in K^p(a_1, \ldots, a_j)$. Suppose that $b_j \in K^p(b_1, \ldots, b_{j-1})$. Then $b_j \in K^p(a_1, \ldots, a_{j-1})$ and

$$c = \prod_{\sigma \in Q} (1 + a_j \sigma(z)^p)^{(\sigma^{-1}x_j)_j} \in K^p(a_1, \ldots, a_{j-1}).$$

Now write $c = f_0 + f_1 a_j + \cdots + f_{p-1}a_j^{p-1}$ where f_i is a polynomial in a_j^p over $\mathbb{Z}_p(\sigma(z)^p \mid \sigma \in Q)$. By Lemma 12 we must have $f_1 = \cdots = f_{p-1} = 0$, so that $c = f_0(a_j^p)$. Just as in the proof of Theorem 11, we can replace a_i by $a_i u$ for infinitely many u in k^p where $k = K^Q$. Hence we can replace a_j by an indeterminate t, so that

$$\prod_{\sigma \in Q} (1 + t\sigma(z)^p)^{(\sigma^{-1}x_j)_j} = f_0(t^p).$$

Differentiate with respect to t and put $t = -1/z^p$ to get a contradiction.

6. Proof of Theorem 5

By Proposition 7 we may assume that H is an abelian p-group, of exponent p^e say. Let R be a Sylow p-subgroup of Q, and denote by $\bar{G}$ the preimage of R under τ. Then the extensions $1 \to H \to G \to Q \to 1$ and $1 \to H \to \bar{G} \to R \to 1$ yield differentials

$$d: H^2(H, K^*)^Q \to H^3(Q, K^*)_p \quad \text{and} \quad \bar{d}: H^2(H, K^*)^R \to H^3(R, K^*)_p.$$

By naturality there is a commutative square

$$\begin{array}{ccc} H^2(H, K^*)^Q & \xrightarrow{d} & H^3(Q, K^*)_p \\ & & \text{res} \\ H^2(H, K^*)^R & \xrightarrow{\bar{d}} & H^3(R, K^*)_p \end{array}$$

Now cor $\circ$ res is simply multiplication by $|Q:R|$, and so res is injective. Therefore

$$\operatorname{Ker} d = \operatorname{Ker} \bar{d} \cap H^2(H, K^*)^Q. \tag{9}$$

We now make a crucial observation about the embedding $\phi: H \to K^*/(K^*)^{p^e}$ provided by Theorem 15. Define S to be the Q-submodule of K^* generated by the elements $1 + a_i z^p$ where $\{a_1, \ldots, a_r\}$ is a suitably chosen p-independent subset. Then (8) shows that ϕ arises from an embedding of H in $S(K^*)^{p^e}/(K^*)^{p^e}$, and hence in S/S^{p^e} since the proof of Theorem 11 shows that $S \cap (K)^{p^e} = S^{p^e}$. So we have in fact constructed an element of the group $\operatorname{Hom}_{\mathbb{Z}_p Q}(H, S/S^{p^e})$, and hence of $\operatorname{Hom}_{\mathbb{Z}_p R}(H, S/S^{p^e})$. Also the latter is isomorphic with $H^2(H, S)^R$ by the proof of Proposition 9.

From the inclusion $S \subseteq K^*$ we obtain the commutative diagram

$$\begin{array}{ccccc} 0 & & 0 & & \\ & & & & \\ \operatorname{Hom}_{\mathbb{Z}_p R}(H, S/S^{p^e}) & \xrightarrow{\sim} & H^2(H, S)^R & \longrightarrow & H^3(R, S) \\ & & & & \\ \operatorname{Hom}_{\mathbb{Z}_p R}(H, K^*/(K^*)^{p^e}) & \xrightarrow{\sim} & H^2(H, K^*)^R & \xrightarrow{\bar{d}} & H^3(R, K^*) \end{array}$$

Now $S/S^p \simeq S(K^*)^p/(K^*)^p$, as $\mathbb{Z}_p Q$-modules, and the latter is free by construction. Therefore S/S^p is $\mathbb{Z}_p R$-free; also S has no p-torsion. Thus we can apply Theorem 6 of [5, p. 143] to conclude that $H^3(R, S) = 0$. Hence ϕ, or rather the corresponding α in $H^2(H, K^*)^Q$, belongs to $\operatorname{Ker} \bar{d}$. Consequently $\alpha \in \operatorname{Ker} d$ by (9). It follows from Lemma 8 that α extends to G and $K_\tau^\alpha G$ is semisimple. □

References

[1] E. Aljadeff and S. Rosset, Global dimensions of crossed products, J. Pure Appl. Algebra 40 (1986) 103–113.

[2] C.W. Curtis and I. Reiner, Methods of Representation Theory, Vol. 1 (Wiley, New York, 1990).

[3] G. Karpilovsky, The Jacobson Radical of Some Classical Rings (Longman, Harlow, UK, 1991).

[4] D. S. Passman, Infinite Crossed Products (Academic Press, San Diego, 1989).

[5] J.-P. Serre, Local Fields (Springer, New York, 1979).

[6] D. Winter, Structure of Fields (Springer, New York, 1978).